Remarks:

The Examiner objected to paragraph 33, line 4 of the specification for containing an undefined acronym. Applicant respectfully points the Examiner to paragraph 32, line 5 of the specification which defines "PAN" as a "personal area network". Accordingly, it is respectfully submitted that the objection to the specification should be withdrawn.

§103 Rejection(s):

Claims 1-15 are rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 6,075,860 A to Ketcham (hereafter "Ketcham") in view of U.S. Patent No. 6,611,913 B1 to Carroll et al (hereafter "Carroll"). Applicant respectfully traverses the rejection.

MPEP §2143 provides: "To establish a prima facie case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations."

Claim 1, as amended, recites a secured communication method for a mobile communications network comprising: "receiving a request to provide a security key to a mobile device connected to the mobile communications network; generating a unique security key for the requesting mobile device using a public or private key mechanism unless the unique security key is preprogrammed into the mobile device; storing the unique security key in a first data structure mechanism in association with a unique value identifying the mobile device; forwarding the unique security key to the mobile device; storing the unique security key in a second data structure mechanism in the mobile device; receiving a request to provide the unique security key for the mobile device to a

service provider; approving the request to provide the unique security key based on content of a list of approved service providers, if a first condition is met, wherein the first condition is set by the mobile device; and providing the unique security key to the service provider, if the service provider is approved to receive the unique security key for the mobile device."

Ketcham fails to disclose the elements of claim 1. Ketcham discloses a method and system for authenticating an authorized user of a remote terminal attempting to connect with a computer network over a wireless modem. The network server and remote terminal exchange encrypted information to authenticate each party. Both the remote terminal and the network server independently generate a data encryption key. [Abstract.] The remote terminal does not retain the user identifier or the authentication encryption key. Instead, an authentication card personal to the authentication card personal to the authorized user is maintained by the authorized user [column 3, lines 61-64]. Ketcham also discloses an authentication database for receiving and storing the user identifier and the authentication encryption key [column 7, lines 17-19] and an account generator that comprises a key generator receptive to an authorization request for generation of a cryptographically suitable authentication encryption key [column 6, lines 48-52].

In particular, Ketcham fails to disclose "receiving a request to provide the unique security key for the mobile device to a service provider; approving the request to provide the unique security key based on content of a list of approved service providers, if a first condition is met, wherein the first condition is set by the mobile device; and providing the unique security key to the service provider, if the service provider is approved to receive the unique security key for the mobile device."

Further, Ketcham teaches away from the elements of claim 1. As provided previously, in Ketcham, the remote terminal does not retain the user identifier or the

authentication encryption key. Instead, an authentication card personal to the authentication card personal to the authorized user is maintained by the authorized user. The second data structure mechanism recited in claim 1, on the other hand, is not personal to an authorized user; the data structure mechanism is tied to the mobile device. For example, the data structure mechanism may store the unique security key in a memory chip in the mobile device [Specification, paragraph 12, line 5]. To a person having ordinary skill in the art, a memory chip, or internal memory, typically cannot be removed from a device without affecting the core functionality of the device.

Carroll also fails to disclose the elements of claim 1. Carroll discloses an escrowed key distribution system and method for authenticating and activating a wireless communication device, where the authentication key is never transmitted over the air. An (escrow) agent randomly generates an authentication key, encrypts the authentication key using a mask, assigns an identifier to the authentication key, and archives the authentication key. The encrypted authentication key and the identifier are inserted into the wireless communication device by the manufacturer of the wireless communication device. [Column 4, lines 22-32.] To activate the wireless communication device, the wireless communication device transmits the identifier to a service provider. The service provider relays the identifier to the agent and, in turn, receives the mask that was used to encrypt the authentication key. Both the service provider and the wireless communication device generate the authentication key independently using an embedded private key algorithm and perform mutual authentication. [Column 4, lines 33-44; column 6, lines 36-45.]

In particular, Carroll fails to disclose "generating a unique security key for the requesting mobile device using a public or private key mechanism unless the unique security key is preprogrammed into the mobile device; …approving the request to provide the unique security key based on content of a list of approved service providers, if a first condition is met, wherein the first condition is set by the mobile device; and

providing the unique security key to the service provider, if the service provider is approved to receive the unique security key for the mobile device."

Additionally, Carroll teaches away from the elements of claim 1. As provided previously, in Carroll, the authentication key is never transmitted over the air. Instead, the service provider uses an identifier and a mask to generate the authentication key. The service provider recited in claim 1, however, may obtain the unique security key upon receiving approval from the mobile device [Specification, paragraph 49, lines 1-3]. Furthermore, also provided previously, the escrowed key distribution system and method in Carroll is limited to an embedded private key algorithm. The secure communication method recited in claim 1, however, may use a public or private key mechanism [Specification, paragraph 44, line 7].

It is respectfully submitted that Ketcham and Carroll combined fail to teach or suggest the elements of claim 1. Carroll fails to cure the deficiencies of Ketcham, and no motivation or reason exists for combining the teachings of Ketcham and Carroll. Ketcham and Carroll combined fail to teach or suggest a secure communication method where a mobile device approves a request to provide a unique security key to a service provider based on content of a list of approved service providers, if a first condition is met, wherein the first condition is set by the mobile device; and provides the unique security key to the service provider, if the service provider is approved to receive the unique security key for the mobile device.

While the suggestion to modify or combine references may come from the knowledge and common sense of a person of ordinary skill in the art, the fact that such knowledge may have been within the province of the ordinary artisan does not in and of itself make it so, absent clear and convincing evidence of such knowledge. *C.R. Bard, Inc. v. M3 Systems, Inc.*, 157 F.3d 1340, 1352, 48 U.S.P.Q.2d 1225, 1232 (Fed. Cir. 1998).

Here, the modification or combination proposed by the Examiner is not based on any clear and convincing evidence of a reason, suggestion, or motivation in the prior art that would have led one of ordinary skill in the art to combine the references. Rather, the reason, suggestion and motivation for the combination of references proposed by the Examiner simply is impermissible hindsight reconstruction given the benefit of Applicant's disclosure.

The Federal Circuit has consistently held that hindsight reconstruction does not constitute a prima facie case of obviousness under 35 U.S.C. § 103. *In re Geiger*, 2 USPQ2d 1276 (Fed Cir. 1987). Unfortunately, the Examiner rather than pointing to what the prior art discloses and teaches as to making the suggested modification relies on assumptions and statements without any support in the record. As such, the Examiner's statements regarding obviousness and motivation to modify are but shortcuts to a conclusion of obviousness devoid of the required analytical approach based on what is actually disclosed in the prior art.

Reliance on impermissible hindsight to avoid express limitations in the claims and setting forth unsupported hypothetical teachings to recreate the Applicant's claimed invention cannot establish a prima facie case of obviousness. Since obviousness may not be established by hindsight reconstruction, the Applicant invites the Examiner to point out the alleged motivation to combine with specificity,[1] or alternatively provide a reference or affidavit in support thereof, pursuant to MPEP §2144.03.[2]

1 *ACS Hospital Systems, Inc. v. Montefiore Hospital*, 221 U.S.P.Q. 929, 933 (Fed. Cir. 1984).

2 "The rationale supporting an obviousness rejection may be based on common knowledge in the art or "well-known" prior art . . . If the applicant traverses such an assertion the examiner should cite a reference in support of his or her position. When a rejection is based on facts within the personal knowledge of the examiner . . . the facts must be supported, when called for by the applicant, by an affidavit from the examiner."

Since no reasonable justification is provided in the Office Action as to how such modification or combination is possible and obviousness may not be established based on hindsight and conjecture, it is respectfully requested that the 103 grounds of rejection be withdrawn.

For the above reasons, neither Ketcham nor Carroll, either alone or in combination, teach or suggest the invention as recited in claim 1. Therefore, it is respectfully submitted that claim 1 is in condition for allowance. Claims 2, 4-6, 8, and 10 depend on claim 1 and should be in condition for allowance by virtue of their dependence on an allowable base claim. Amended claim 11 substantially incorporates the elements of claim 1; therefore, claim 11 should also be in condition for allowance.

No amendment made was related to the statutory requirements of patentability unless expressly stated herein; and no amendment made was for the purpose of narrowing the scope of any claim, unless Applicants have expressly argued herein that such amendment was made to distinguish over a particular reference or combination of references.

If for any reason the Examiner finds the application other than in condition for allowance, the Examiner is requested to call the undersigned attorney at the Los Angeles, California, telephone number (310) 789-2100 to discuss the steps necessary for placing the application in condition for allowance.

Respectfully submitted,

/F. Jason Far-hadian/

Date: November 16, 2007

By: _____

F. Jason Far-hadian, Esq.
Registration No. 42,523